

FCC Mail Room

EB Docket 06-36

Title of signatory: CEO

Date _____

No. of Copies rec'd.
Line ABCDE

Attachment A
Statement of CPNI Procedures and Compliance

Statement of CPNI Procedures and Compliance

Use of CPNI

SoundConnect does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. SoundConnect has trained its personnel not to use CPNI for marketing purposes. Should SoundConnect elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

PROTECTION OF CPNI

SoundConnect has put into place processes to safeguard its customers' CPNI from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI.

SoundConnect provides audio & web conferencing services to business customers. Therefore, SoundConnect customer's call detail records only include the phone number dialed from, but does not include the phone number dialed since all calls terminate to a central/hosted conference bridge.

DISCLOSURE OF CALL DETAIL OVER PHONE

SoundConnect has instituted authentication procedures to safeguard the disclosure of call detail over the telephone. SoundConnect's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. Customers wishing to have access to billing information over the phone are required to establish a password and security question. The policy is the same regardless if the call is initiated by SoundConnect or the customer.

SoundConnect has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. SoundConnect's back-up authentication procedure operates as follows: The customer must provide a correct answer to the security question when prompted and only then will SoundConnect send a new, temporary password to the email address associated with the account.

SoundConnect has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information.

DISCLOSURE OF CPNI ONLINE

SoundConnect has instituted authentication procedures to safeguard the disclosure of CPNI on-line. SoundConnect's authentication procedures do not require the use of

readily available biographical information or account information as defined by the FCC. Customers wishing to have online access to billing information are required to establish a password and security question, without the use of readily available biographical information or account information, at the time of account set up. Unless the appropriate password is provided, SoundConnect does not allow on-line access to CPNI.

SoundConnect has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. SoundConnect's back-up authentication procedure operates as follows: The customer must provide a correct answer to the security question when prompted and only then will SoundConnect send a new, temporary password to the email address associated with the account,

SoundConnect has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information.

NOTIFICATION TO LAW ENFORCEMENT

Company has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. SoundConnect will provide electronic notification of breach of CPNI within seven business days to the United States Secret Service and the Federal Bureau of Investigation. SoundConnect will wait another full seven business days before notifying the affected customers of the breach unless otherwise directed by the relevant investigating agency.

SoundConnect maintains electronic records of all breaches discovered and notifications made to the USSS and the FBI, and to customers. Records of discovered breaches will be maintained for at least two years.

SoundConnect takes every reasonable precaution to protect the confidentiality of proprietary or personal customer information including secure storage of data, CPNI policy training for all employees with access to data, and strict adherence to the method and authorization required for release of CPNI.

ACTIONS AGAINST DATA BROKERS

Company has not taken any actions against data brokers in the last year.

CUSTOMER COMPLAINTS ABOUT CPNI BREACHES

Company did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2011.

INFORMATION ABOUT PRETEXTERS

Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI but does take steps to diligently protect CPNI.